

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
12 May 2005 (12.05.2005)

PCT

(10) International Publication Number
WO 2005/043805 A1

(51) International Patent Classification⁷: **H04L 9/08**

(21) International Application Number:
PCT/IB2004/052235

(22) International Filing Date: 28 October 2004 (28.10.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/515,319 29 October 2003 (29.10.2003) US
60/561,605 13 April 2004 (13.04.2004) US

(71) Applicant (for all designated States except US): KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor; and

(75) Inventor/Applicant (for US only): VAN DIJK, Marten, E. [US/US]; P.O. Box 3001, Briarcliff Manor, NY 10510-8001 (US).

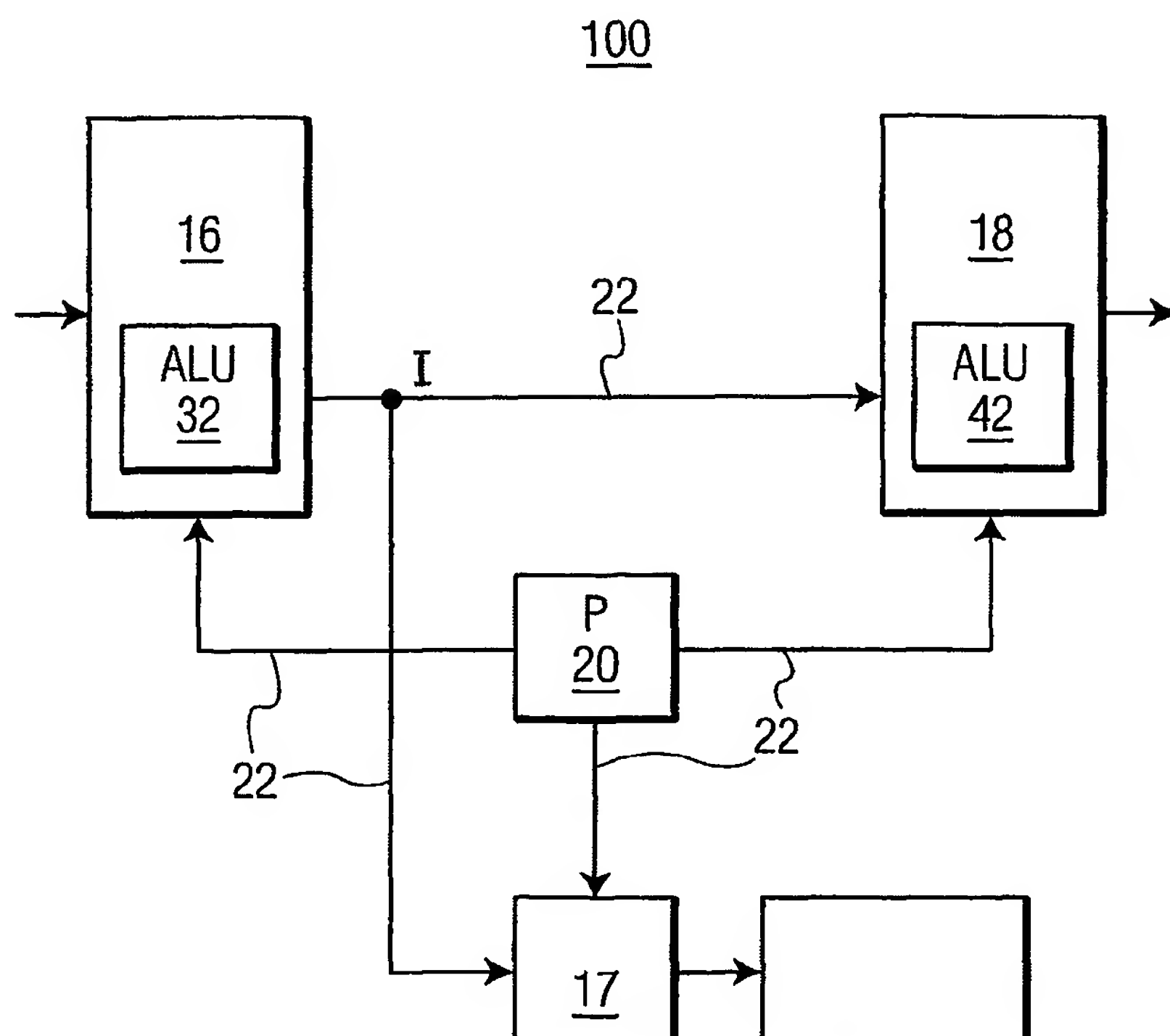
(74) Common Representative: KONINKLIJKE PHILIPS ELECTRONICS N.V.; Intellectual Property & Standards, c/o HALAJIAN, Dicran P.O. Box 3001, Briarcliff Manor, NY 10510-8001 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI,

[Continued on next page]

(54) Title: SYSTEM AND METHOD OF RELIABLE FORWARD SECRET KEY SHARING WITH PHYSICAL RANDOM FUNCTIONS



(57) Abstract: A secure solution is provided to the problem of secret key agreement. In particular, a method of reliable forward secret key sharing is disclosed between two legitimate correspondents whose profiles match sufficiently. The invention relies on a physical random function, sometimes referred to as a physical unclonable function (PUF) to provide a secure solution to the problem of secret key agreement. In one embodiment, a one-pass protocol is introduced based on Reed-Solomon codes leading to an unconditionally secure solution. In a further embodiment, the solution of the first embodiment is improved upon by providing a conditionally secure solution based on a pseudo random family of functions. In a still further embodiment, a two-pass protocol is introduced which is used exclusively for purposes of identification and authentication. In accordance with the principles of the two-pass protocol, two communications are required and unlike the one-pass protocol, the second correspondent selects the secret key K.



SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ,*

BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

- *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for all designations*

Published:

- *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.